www.GossamerSec.com

Assurance Activity Report for Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.10

Version 1.1
05/19/14

Prepared by:
Gossamer Security Solutions
Accredited Security Testing Laboratory – Common Criteria Testing
Catonsville, MD 21228

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Revision History

Revision	Date	Authors	Summary
Version 1.0	02/14/14	Arnold/Compton	Initial draft
Version 1.1	05/19/14	Compton	Updated document versions

The TOE Evaluation was sponsored by:

Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134

Evaluation Personnel:

- James Arnold
- Tammy Compton

Common Criteria Versions:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Table of Contents

1. Introduction 5
2. Protection Profile SFR Assurance Activities 6
   - 2.1 Security audit (FAU) 6
     - 2.1.1 Audit Data Generation (FAU_GEN.1) 6
     - 2.1.2 User identity association (FAU_GEN.2) 14
     - 2.1.3 External Audit Trail Storage (FAU_STG_EXT.1) 14
   - 2.2 Cryptographic support (FCS) 16
     - 2.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1) 16
     - 2.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4) 17
     - 2.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1)) 18
     - 2.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2)) 19
     - 2.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3)) 19
     - 2.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4)) 20
     - 2.2.7 Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1) 21
     - 2.2.8 Explicit: SSH (FCS_SSH_EXT.1) 23
     - 2.2.9 Explicit: TLS (FCS_TLS_EXT.1) 27
   - 2.3 User data protection (FDP) 28
     - 2.3.1 Full Residual Information Protection (FDP_RIP.2) 28
   - 2.4 Identification and authentication (FIA) 28
     - 2.4.1 Password Management (FIA_PMG_EXT.1) 28
     - 2.4.2 Protected Authentication Feedback (FIA_UAU.7) 29
     - 2.4.3 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2) 30
     - 2.4.4 User Identification and Authentication (FIA_UIA_EXT.1) 31
   - 2.5 Security management (FMT) 32
     - 2.5.1 Management of TSF Data (for general TSF data) (FMT_MTD.1) 32
     - 2.5.2 Specification of Management Functions (FMT_SMF.1) 34
     - 2.5.3 Restrictions on Security Roles (FMT_SMR.2) 35
   - 2.6 Protection of the TSF (FPT) 37

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.6.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1) 37
2.6.2 Extended: Protection of TSF Data (for reading of all symmetric keys) (FPT_SKP_EXT.1) 38
2.6.3 Reliable Time Stamps (FPT_STM.1) 38
2.6.4 TSF Testing (FPT_TST_EXT.1) 39
2.6.5 Extended: Trusted Update (FPT_TUD_EXT.1) 40
2.7 TOE access (FTA) 42
2.7.1 TSF-initiated Termination (FTA_SSL.3) 42
2.7.2 User-initiated Termination (FTA_SSL.4) 42
2.7.3 TSF-initiated Session Locking (FTA_SSL_EXT.1) 43
2.7.4 Default TOE Access Banners (FTA_TAB.1) 43
2.8 Trusted path/channels (FTP) 44
2.8.1 Inter-TSF trusted channel (FTP_ITC.1) 44
2.8.2 Trusted Path (FTP_TRP.1) 46
3. Protection Profile SAR Assurance Activities 49
3.1 Development (ADV) 49
3.1.1 Basic functional specification (ADV_FSP.1) 49
3.2 Guidance documents (AGD) 49
3.2.1 Operational user guidance (AGD_OPE.1) 49
3.2.2 Preparative procedures (AGD_PRE.1) 50
3.3 Life-cycle support (ALC) 51
3.3.1 Labelling of the TOE (ALC_CMC.1) 51
3.3.2 TOE CM coverage (ALC_CMS.1) 51
3.4 Tests (ATE) 51
3.4.1 Independent testing - conformance (ATE_IND.1) 51
3.5 Vulnerability assessment (AVA) 52
3.5.1 Vulnerability survey (AVA_VAN.1) 52

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

1. Introduction

This document presents evaluations results of the Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.10 Protection Profile for Network Devices (NDPP) evaluation. This document contains a description of the assurance activities and associated results as performed by the evaluators.

Note that this report is based on the Protection Profile for Network Devices, version 1.1, 8 June 2012 with Errata#2.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2. Protection Profile SFR Assurance Activities

This section of the ETR identifies each of the assurance activities included in the claimed Protection Profile and describes the findings in each case.

The following evidence was used to complete the Assurance Activities:

AA report v1.1

- Brocade Communications Systems, Inc. FastIron SX, ICX, and FCX Series Switch/Router 8.0.10 Security Target, Version 1.0, May 19, 2014.
- Brocade FastIron FIPS Configuration Guide Supporting FastIron Software Release 08.0.10, 53-1003198-02, 9 May 2014 (FastIron_FIPS_08010_ConfigGuide.pdf)
- Brocade FastIron Ethernet Switch Security Configuration Guide Supporting FastIron Software Release 08.0.10, 53-1003088-01, 8 January 2014 (FastIron_08010_SecurityGuide.pdf)
- Brocade FastIron Ethernet Switch Administration Guide Supporting FastIron Software Release 08.0.10, 53-1003075-01, 8 January 2014 (FastIron_08010_AdminGuide.pdf)

2.1 Security audit (FAU)

2.1.1 Audit Data Generation (FAU_GEN.1)

2.1.1.1 FAU_GEN.1.1

TSS Assurance Activities: **For protocol related audit events:** The evaluator shall check to ensure that the TSS contains a list (possibly empty except for authentication failures for user-level connections) of the protocol failures that are auditable.

Section 6.1 references the table of audit events in the SFR. The reference is a list of events, including protocol failures, starting and stopping the audit function, administrator commands, and authentication events.

Guidance Assurance Activities: The evaluator shall check the administrative guide and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN1.2, and the additional information specified in Table 1 **of the NDPP**.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP. The evaluator shall examine the administrative guide and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to this PP. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.

Requirement	Auditable Events	Additional Audit Record Contents	Guidance Location
FAU_GEN.1	Startup of audit		FIPS Configuration Guide, Appendix B Informational Message Logging CLI_CMD operation enabled by *user* from console session. "logging cli-command" by *user* from console
FAU_GEN.1	Shutdown of audit		FIPS Configuration Guide, Appendix B Informational Message Logging CLI_CMD operation disabled by *user* from console session
FCS_SSH_EXT.1	Failure to establish an SSH session. Establishment/Termination of an SSH session. [1]	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.	Administration Guide, Appendix A Informational Message telnet | SSH| access [by username] from src IP source ip address , src MAC source MAC address rejected, n attempts access attempts from the specified source IP and MAC address. • [by user *username*] does not appear if telnet or SSH clients are specified. • *n* is the number of times this SNMP trap occurred in the last five minutes, or other configured number of minutes.
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session. [1]	Reason for failure. Non-TOE endpoint of connection (IP address) for	FIPS Configuration Guide, Appendix B Informational Message SSL Syslog server ip-address:portnum is now disconnected

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Requirement	Auditable Events	Additional Audit Record Contents	Guidance Location
		both successes and failures.	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	Console: Success Administration Guide, Appendix A Informational Message Security: console login by *username* to USER | PRIVILEGE EXEC mode The specified user logged into the device console into the specified EXEC mode. Failure: FIPS Configuration Guide, Appendix B Informational Message Error - Incorrect username or password in console session SSH: Success Administration Guide, Appendix A Informational Message Security: telnet | SSH login by *username* from src IP *ip-address*, src MAC *mac-address* to USER | PRIVILEGE EXEC mode The specified user logged into the device using Telnet or SSH from either or both the specified IP address and MAC address. The user logged into the specified EXEC mode Failure Administration Guide, Appendix A Informational Message telnet | SSH | from src IP source *ip address*, src MAC *source MAC address* rejected, *n* attempts access attempts from the specified source IP and MAC address. • [by user *username*] does not appear if telnet or SSH clients are specified. • *n* is the number of times this SNMP trap occurred in the last five minutes, or other configured number of

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Requirement	Auditable Events	Additional Audit Record Contents	Guidance Location
			minutes. TLS: FIPS Configuration Guide, Appendix B Informational Message *SSL Syslog server ip-address:portnum is now connected* Failure FIPS Configuration Guide, Appendix B Informational Message SSL Syslog server *ip-address:portnum* is now disconnected.
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	See FIA_UIA_EXT.1
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).	FIPS Configuration Guide, Appendix B Alert Message Time is updated by NTP server *ip-address* from NO_CLOCK to <*new time*> GMT+00 <*new date*> Clock Changed from old time <*old time*> GMT+00 <*old date*> to new time <*new time*> GMT+00 <*new date*>
FPT_TUD_EXT.1	Initiation of update.	No additional information.	Administration Guide, Appendix A Informational Message startup-config was changed or startup-config was changed by *user-name* A configuration change was saved to the startup-config file. The *user-name* is the user ID, if they entered a user ID to log in.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.	Administration Guide, Appendix A Informational Message Security: console logout by *username*

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Requirement	Auditable Events	Additional Audit Record Contents	Guidance Location
			The specified user logged out of the device console
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.	FIPS Configuration Guide, Appendix B Informational Message SSH session for *user* from src IP *ip-address*, MAC *mac-address* in PRIVILEGED EXEC mode has timed out.
FTA_SSL.4	The termination of an interactive session.	No additional information.	Administration Guide, Appendix A Informational Message Security: console logout by *username* The specified user logged out of the device console
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	See SSH and TLS event types.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.	See SSH event type
FMT_SMF.1 (Administrator actions)	Changes to the audit configuration		FIPS Configuration Guide, Appendix B Informational Message SSL Syslog server *ip-address:portnum* is now connected. OR SSL Syslog server *ip-address:portnum* is now disconnected A user made Syslog configuration changes to the specified Syslog server address, or enabled or disabled a Syslog operation through the Web, SNMP, console, SSH, or Telnet session FIPS Configuration Guide, Appendix B Informational Message

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Requirement	Auditable Events	Additional Audit Record Contents	Guidance Location
			Logging CLI_CMD operation enabled by *user* from console session. "logging cli-command" by *user* from console Logging CLI_CMD operation disabled by *user* from console session Note: All CLI commands are recorded with the CLI_CMD event type
	User Account creation and password management		Administration Guide, Appendix A Informational Message user *username* added | deleted | modified from console | telnet | ssh | web | snmp A user created, modified, or deleted a local user account through the Web, SNMP, console, SSH, or Telnet session Security: Password has been changed for user *username* from *session-id* Password of the specified user has been changed during the specified session ID or type. *session-id* can be console, telnet, ssh, web, or snmp.
	Login policy management (time restrictions, minimum password length)		The CLI_CMD event type records all administrator commands from the CLI interface. All login policy changes are recorded using this event type Logging CLI_CMD operation enabled by *user* from console session. "logging cli-command" by *user* from console
	ALC management		Administration Guide, Appendix A Informational Message ACL *ACL id* added | deleted | modified from console | telnet | ssh | web | snmp session A user created, modified, deleted, or applied an ACL through a Web, SNMP, console, SSH, or Telnet session
	Enabling FIPS mode		The CLI_CMD event type records all administrator commands from the CLI interface. Changes to the FIPS mode are

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Requirement	Auditable Events	Additional Audit Record Contents	Guidance Location
			recorded using this event type Logging CLI_CMD operation enabled by *user* from console session. "logging cli-command" by *user* from console

The following commands were identified by the evaluators as security-related. Each command is identified and a brief purpose is provided. These commands were found in the user guidance and consist of all the commands needed to configure or examine the security settings through the process of testing the security claims. This same list is found in Section 6.5 of the ST. As such, they are all identified in the DTR, along with the results and corresponding audit records. Note that every administrator command issued by the evaluators during testing was found to be audited without exception.

- fips
  - (no) fips enable common-criteria (turn fips and cc modes on or off)
  - fips show (show the current fips configuration)
- write memory (write the current configuration settings to persistent memory)
- openssl s_server (set syslog port, key and cipher)
- (no) logging host <ip-address> ssl-port <port> (configure or remove the secure logging host)
- ip
  - ip ssh pub-key-file (load a user's public key for authentication)
  - ip ssh idle-time <time> (set SSH idle timeout period)
- aaa authentication (configure authentication settings)
- enable
  - enable aaa (enable login at console)
  - enable password-min-length 15 (configure min password size)
  - enable user password-masking (set as part of turning on FIPS mode)
- username <user> password (set a user password)
- clock set <time> (set time)
- server <ntp server ip> minpoll <time> (configure NTP poll interval)
- show
  - show flash (show flash info)
  - show ver (show version)
  - show clock (query time)
  - show ip client-pub-key (show the client public key used for SSH login)
  - show ip ssl (show ssl connections)
  - show logging (show current logging configuration and log buffer)
  - show run | <options> (show running configuration details)
- boot system flash <primary or secondary> (boot a loaded flash image)

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

- console timeout <time> (set console idle timeout period)
- banner motd + (set the login banner – message of the day)
- exit (logout or exit current shell)
- ntp (switch to ntp configuration mode)
- config t (switch to configuration mode)

Testing Assurance Activities: The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in table 1 **of the NDPP** and administrative actions. This should include all instances of an event--for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. For administrative actions, the evaluator shall test that each action determined by the evaluator above to be security relevant in the context of this PP is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

For protocol related audit events: The evaluator shall test all identified audit events during protocol testing/audit testing.

The evaluator created a mapping for the required audit events to test cases where the associated function was tested. The evaluator then collected the audit event when running the security functional tests. For example, the required event for FCS_SSH.1 is Establishment/Termination of an SSH session. The evaluator collected these audit records when establishing the SSH sessions to test password based authentication for SSH and recorded them in the Detailed Test Report (DTR). The security management events are handled in a similar manner. When the administrator was required to set a value for testing, the audit record associated with the administrator action was collected and recorded in the DTR.

2.1.1.2 FAU_GEN.1.2

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Testing Assurance Activities: None Defined

2.1.2 User identity association (FAU_GEN.2)

2.1.2.1 FAU_GEN.2.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.1.3 External Audit Trail Storage (FAU_STG_EXT.1)

2.1.3.1 FAU_STG_EXT.1.1

TSS Assurance Activities: For both types of TOEs (those that act as an audit server and those that send data to an external audit server), there is some amount of local storage. The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server (for TOEs that are not acting as an audit log server). For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

TOE acts as audit server

The evaluator shall examine the TSS to ensure it describes the connection supported from non-TOE entities to send the audit data to the TOE, and how the trusted channel is provided.

TOE is not an audit server

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.

Section 6.1 explains how the audit trail is protected. Only the TOE User role can access the audit trail and use of that role requires a valid logon. Only administrators log onto the TOE. Section 6.1 also explains there is a local audit log and the possibility of a remote audit log. The local log stores up to 50 entries after which the audit entries will be overwritten, oldest first. The administrator (with Super User privilege) can choose to configure one or more external syslog servers where the TOE will send a copy of the audit records if so desired. The TOE can be configured to use TLS to protect audit logs exported to an external server.

Guidance Assurance Activities: **TOE acts as audit server**

The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel with the TOE, as well as describe any requirements for other IT entities to connect and send audit data to the TOE (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with other IT entities.

TOE is not an audit server

The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.

Appendix A of the **FIPS Configuration Guide** provides detailed instructions for configuring the SSL/TLS connection between the TOE and the audit server. The commands provided are for the Ubuntu 10.4 audit server. The reader is told that the TOE will work with Red Hat or Centos but the commands are slightly different (and left to the reader). The steps provide are as follows. Each major step has several sub-steps explained.

- Set up stunnel
- Create a certificate with the openssl tool
- Create a configuration file
- Change the stunnel4 startup file
- Restart the stunnel service
- Configure rsyslog
- Enable accepting remote logs
- Restart rsyslog service
- Print log messages

Testing Assurance Activities: **TOE acts as audit server**

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.

The evaluator shall perform the following test for this requirement:

Test 1: The evaluator shall establish a session between an external IT entity and the TOE according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the IT entity and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the TOE. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the TOE. The evaluator shall perform this test for each protocol selected in the second selection.

TOE is not an audit server

Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.

The evaluator shall perform the following test for this requirement:

Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.

The evaluator followed the procedures in the FIPS Guide, Appendix A for setting up the syslog server connection. The audit server tested was CentOS release 6.4 (Final) Kernel 2.6.32-358.11.1.el6.x86_64 on an x86_64. The evaluator used Wireshark to observe the traffic between the TOE and the audit log server. The evaluator was able to establish a connection with each of the claimed TLS ciphers while performing this test. The evaluator used the syslog server to store audit as recommended by the Brocade for the duration of testing so many audit records were recorded during the course of testing.

2.2 Cryptographic support (FCS)

2.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1)

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.2.1.1 FCS_CKM.1.1

TSS Assurance Activities: The evaluator shall ensure that the TSS contains a description of how the In order to show that the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.

Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described

FCS_CKM.1.1 selected ***NIST Special Publication 800-56B***, so the evaluator expected to find only that publication addressed in the TSS.

Section 6.2, Table 6, addresses SP 800-56B with section references, indications of whether identified features are implemented and where the implementation disagrees with the recommendation a rationale is provided. Note that no such deviations are identified.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall use the key pair generation portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and either "The RSA Validation System (RSAVS)" (for FIPS 186-2) or “The 186-3 RSA Validation System (RSA2VS)” (for FIPS 186-3) as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

The TOE has been FIPS approved. The RSA certificate numbers are 1396, 1388, 1391, 1386, and 1387 covering all evaluated models.

2.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

2.2.2.1 FCS_CKM_EXT.4.1

TSS Assurance Activities: The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").

Section 6.2, a list is presented (after Table 11) that identifies secret keys, private keys, and CSPs with a brief summary of purpose. Following the list, is a description of where keys are stored and when and how they are destroyed.

1. **Describe each secret key, private key, and CSP:** The list identified above serves to describe each key to some degree.
2. **When they are zeroized:** The paragraph following the list identified above indicates they are destroyed when no longer needed and that is followed up with more detail in some cases.
3. **Type of zeroization procedure:** The paragraph following the list identified above indicates that in FLASH values are either overwritten once with zeros or overwritten with a new value. In RAM values are overwritten once with zeroes.

The TSS includes a table identifying whether keys and CSPs reside in FLASH or RAM. The description cited above has been clarified to indicate that persistent values are stored in FLASH.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

2.2.3.1 FCS_COP.1(1).1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

The TOE has been FIPS approved. The AES certificate numbers are 2697, 2688, 2690, 2686, and 2687covering all evaluated models.

2.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

2.2.4.1 FCS_COP.1(2).1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSA2VS), and "The RSA Validation System" (RSAVS (for 186-2) or RSA2VS (for 186-3)) as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e., FIPS PUB 186-2 or FIPS PUB 186-3). This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

The TOE has been FIPS approved. The RSA certificate numbers are 1396, 1388, 1391, 1386, and 1387 covering all evaluated models.

2.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.2.5.1 FCS_COP.1(3).1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

The TOE has been FIPS approved. The SHA certificate numbers are 2265, 2259, 2260, 2257, 2258 covering all evaluated models.

2.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4))

2.2.6.1 FCS_COP.1(4).1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

The TOE has been FIPS approved. The HMAC certificate numbers are 1679, 1675, 1676, and 1674 covering all evaluated models.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.2.7 Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1)

2.2.7.1 FCS_RBG_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.2.7.2 FCS_RBG_EXT.1.2

TSS Assurance Activities: Documentation shall be produced—and the evaluator shall perform the activities—in accordance with Annex D, Entropy Documentation and Assessment **of the NDPP**.

The Entropy description is provided in a separate (non-ST) document that has been delivered to CCEVS for approval. Note that the entropy analysis has been accepted by CCEVS/NSA.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms.

Implementations Conforming to FIPS 140-2, Annex C

The reference for the tests contained in this section is The Random Number Generator Validation System (RNGVS) [RNGVS]. The evaluator shall conduct the following two tests. Note that the 'expected values' are produced by a reference implementation of the algorithm that is known to be correct. Proof of correctness is left to each Scheme.

The evaluator shall perform a Variable Seed Test. The evaluator shall provide a set of 128 (Seed, DT) pairs to the TSF RBG function, each 128 bits. The evaluator shall also provide a key (of the length appropriate to the AES algorithm) that is constant for all 128 (Seed, DT) pairs. The DT value is incremented by 1 for each set. The seed values shall have no repeats within the set. The evaluator ensures that the values returned by the TSF match the expected values.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

The evaluator shall perform a Monte Carlo Test. For this test, they supply an initial Seed and DT value to the TSF RBG function; each of these is 128 bits. The evaluator shall also provide a key (of the length appropriate to the AES algorithm) that is constant throughout the test. The evaluator then invokes the TSF RBG 10,000 times, with the DT value being incremented by 1 on each iteration, and the new seed for the subsequent iteration produced as specified in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3. The evaluator ensures that the 10,000th value produced matches the expected value.

Implementations Conforming to NIST Special Publication 800-90

The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RBG functionality.

If the RBG has prediction resistance enabled, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. “generate one block of random bits” means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).

If the RBG does not have prediction resistance, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

- Entropy input: the length of the entropy input value must equal the seed length.
- Nonce: If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.
- Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

- Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

The Entropy description is provided in a separate (non-ST) document that has been delivered to CCEVS for approval. Note that the entropy analysis has been accepted by CCEVS/NSA.

The TOE has been FIPS approved. The CTR_DRBG certificate numbers are 442, 438, 439, 436, 437 covering all evaluated models.

2.2.8 Explicit: SSH (FCS_SSH_EXT.1)

2.2.8.1 FCS_SSH_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.2.8.2 FCS_SSH_EXT.1.2

TSS Assurance Activities: The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSH_EXT.1.5, and ensure that password-based authentication methods are also allowed.

Section 6.2 indicates the SSH implementation supports AES CBC 128 and 256, HMAC-SHA-1, and RSA. These values match the SFR. Section 6.2 also indicates that both public-key and password based authentication can be configured.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall also perform the following tests:

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.

Test 2: Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.

The evaluator used the Putty client to connect to the TOE using password authentication. The evaluator performed this test using ASE 128 and ASE 256 encryption.

2.2.8.3 FCS_SSH_EXT.1.3

TSS Assurance Activities: The evaluator shall check that the TSS describes how 'large packets' in terms of RFC 4253 are detected and handled.

Section 6.2 explains that there is a 256K packet buffer and as SSH packets are received they are combined to form a complete packet to be decrypted, but if the packet is not completed when the buffer becomes full the packet will be dropped.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall also perform the following test:

Test 1: The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.

The evaluator created a test program that sends a packet of length 257K to the SSH server on the TOE. When the large packet was sent to the TOE, the SSH connection was closed.

2.2.8.4 FCS_SSH_EXT.1.4

TSS Assurance Activities: The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Section 6.2 indicates the SSH implementation supports AES CBC 128 and 256, HMAC-SHA-1, and RSA. These values match the SFR. The description also indicates that a maximum packet size of 256K is supported and that is also consistent with the SFR.

Guidance Assurance Activities: The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

The ST identifies the ciphers, hashes, and authentication methods as indicated in the TSS findings above.

The FIPS Configuration Guide in the "Supported algorithms for SSH Client " section states that aes128-cbc and aes256-cbc are the only permitted cipher suites. The TOE gets set in Common Criteria mode so the evaluator assumes the algorithms are limited when the mode is set.

Testing Assurance Activities: The evaluator shall also perform the following test:

Test 1: The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

The evaluator used the SecureCRT client to connect to the TOE using ASE 128 and ASE 256 encryption. The evaluator captured the network traffic and verified the algorithms.

2.2.8.5 FCS_SSH_EXT.1.5

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.2.8.6 FCS_SSH_EXT.1.6

TSS Assurance Activities: The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that that list corresponds to the list in this component.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Section 6.2 indicates the SSH implementation supports AES CBC 128 and 256, HMAC-SHA-1, and RSA. These values match the SFR. The description also indicates that a maximum packet size of 256K is supported and that is also consistent with the SFR.

Guidance Assurance Activities: The evaluator shall also check the operational guidance to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).

The ST identifies the ciphers, hashes, and authentication methods as indicated in the TSS findings above.

Section 2 of the **Security Configuration Guide** in the **SSH2 supported features** section indicates that the following hashes are supported: hmac-sha1. As such, it seems the only available hash matches that in the ST and no specific instructions are necessary.

Testing Assurance Activities: The evaluator shall also perform the following test:

Test 1: The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

This test was completed in conjunction with FCS_SSH_EXT.1.5. The evaluator used the SecureCRT client to connect to the TOE using ASE 128 and ASE 256 encryption and hmac-sha1 (the only applicable integrity algorithm). The evaluator captured the network traffic and verified the algorithm.

2.2.8.7 FCS_SSH_EXT.1.7

TSS Assurance Activities: If this capability is "hard-coded" into the TOE, the evaluator shall check the TSS to ensure that this is stated in the discussion of the SSH protocol.

Section 6.2 indicates that DH14 is a supported key exchange method. It also states that other ciphers are implemented but they are disabled while operating in CC and FIPS mode.

Guidance Assurance Activities: The evaluator shall ensure that operational guidance contains configuration information that will allow the security administrator to configure the TOE so that all key exchanges for SSH are performed using DH group 14.

The ST identifies the ciphers, hashes, and authentication methods as indicated in the TSS findings above.

The **FIPS Configuration Guide** in section **Features unavailable in Common Criteria mode** states that for SSH key exchange method DiffieHellmanGroup1Sha1 is not supported. Only DiffieHellmanGroup14Sha1 is supported

Testing Assurance Activities: The evaluator shall also perform the following test:

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Test 1: The evaluator shall attempt to perform a diffie-hellman-group1-sha1 key exchange, and observe that the attempt fails. For each allowed key exchange method, The evaluator shall then attempt to perform a key exchange using that method, and observe that the attempt succeeds.

The evaluator was able to observe from previous tests that diffie-hellman-group14-sha1 key exchange was used in all negotiations. The evaluator attempted a diffie-hellman-group1-sha1 key exchange and the request was rejected.

2.2.9 Explicit: TLS (FCS_TLS_EXT.1)

2.2.9.1 FCS_TLS_EXT.1.1

TSS Assurance Activities: The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

The SFR claims only the required 4 ciphers and those are identified in section 6.2 of the TSS. Section 6.2 also indicates that TLSv1.0 is supported, matching the SFR claim.

Guidance Assurance Activities: The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

The ST indicates that TLSv1.0 is supported and identifies the following required ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, and TLS_DHE_RSA_WITH_AES_256_CBC_SHA.

The **FIPS Configuration Guide – How FIPS Works** indicates that the fips enable instruction places the TOE into FIPS mode. Once in FIPS mode, that section indicates that SSL3.0 is disabled and only TLSv1.0 or greater can be used with the TOE.

The **FIPS Configuration Guide** in the "Supported cipher suites" section lists the TLS cipher suites as: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, and TLS_DHE_RSA_WITH_AES_256_CBC_SHA. This list matches those provided in the ST.

Testing Assurance Activities: The evaluator shall also perform the following test:

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

The connection between the syslog server and the TOE is secured using TLS. The evaluator established a connection between the two machines using each of the claimed ciphersuites.

2.3 User data protection (FDP)

2.3.1 Full Residual Information Protection (FDP_RIP.2)

2.3.1.1 FDP_RIP.2.1

TSS Assurance Activities: 'Resources' in the context of this requirement are network packets being sent through (as opposed to 'to', as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.

Section 6.3 indicates that when packets are sent they are placed in a buffer pool and subsequently overwritten. If a packet exceeds the size of a buffer, the residual space is overwritten with zeros (i.e., padded).

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.4 Identification and authentication (FIA)

2.4.1 Password Management (FIA_PMG_EXT.1)

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.4.1.1 FIA_PMG_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators on the composition of strong passwords, and that it provides instructions on setting the minimum password length.

The **Enabling enhanced user password combination requirements** section of the **Security Configuration Guide** describes how to turn on strict password enforcement**.** When strict-password-enforcement is on, passwords must be eight characters and contain:

- At least two upper case characters
- At least two lower case characters
- At least two numeric characters
- At least two special characters

There is a section of the **Security Configuration Guide** called **Specifying a minimum password length** that explains the command needed to set a minimum password length.

Testing Assurance Activities: The evaluator shall also perform the following tests. Note that one or more of these tests can be performed with a single test case.

Test 1: The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.

The evaluator ran three tests to address this requirement. The first step had the administrator set the minimum password length to 15. The first test has 14 characters including those to meet the strict enforcement and failed. The second test had 15 characters including those to meet the strict enforcement and passed. The last test included all the claimed special characters and passed. The evaluator felt this sample was adequate because the minimum settable length was tested and the combination of password characters was included.

2.4.2 Protected Authentication Feedback (FIA_UAU.7)

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.4.2.1 FIA_UAU.7.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall perform the following test for each method of local login allowed:

Test 1: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.

The evaluator observed during testing that passwords are obscured on the console login.

2.4.3 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2)

2.4.3.1 FIA_UAU_EXT.2.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: Assurance activities for this requirement are covered under those for FIA_UIA_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA_UIA_EXT.1.

All authentication mechanisms are included in the testing for FIA_UIA_EXT.1.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.4.4 User Identification and Authentication (FIA_UIA_EXT.1)

2.4.4.1 FIA_UIA_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.4.4.2 FIA_UIA_EXT.1.2

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon".

Section 6.4 describes that the TOE supports password authentication and can be configured on a per user basis to support (i.e., by uploading the user's public key) SSH public-key-based authentication mechanisms. Administrators define and assign attributes to users and those determine the privileges the user will have once logged on. The ST states that the TOE presents the user with a command prompt constitutes a successful login.

The evaluator shall examine the operational guidance to determine that any necessary preparatory steps (e.g., establishing credential material such as pre-shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the operational guidance provides clear instructions

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the operational guidance provides sufficient instruction on limiting the allowed services.

The **Local user accounts** section of the **Security Configuration Guide** discusses the different logon options. It clearly describes that a username and password are required for logging into the machine. The **SSH2 authentication types** section of the **Security Configuration Guide** explains how to setup and use SSH authentication. It describes the process for creating a public-private key pair and how to provide the public key to the user. **The Configuring DSA or RSA challenge-response authentication** section provides a step by step process of the authentication process with SSH.

The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:

Test 1: The evaluator shall use the operational guidance to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.

Test 2: The evaluator shall configure the services allowed (if any) according to the operational guidance, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.

Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.

The evaluator configured the TOE for local console access and for remote SSH access. The evaluator then performed an unsuccessful and successful logon of each type using bad and good credentials respectively. The evaluator was able to observe the TOE routed traffic on the traffic and it displayed a banner to the user before login. No functions were available to the administrator accessing the console with the exception of acknowledging the banner.

2.5 Security Management (FMT)

2.5.1 Management of TSF Data (for general TSF data) (FMT_MTD.1)

2.5.1.1 FMT_MTD.1.1

TSS Assurance Activities: The evaluator shall examine the TSS to determine that, for each administrative function identified in the operational guidance; those that are accessible through an interface prior to administrator log-in

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.

Section 6.4 indicates that the TOE doesn't offer any functions prior to logging in.

Section 6.5 explains that there are privilege levels and the Super User privilege is used to denote an Authorized Administrator. The TSF data manipulation commands are restricted to that privilege level.

See FMT_SMF.1. The evaluator has found guidance for each of the identified management functions. All management functions are available only after having logged in and if the user has the appropriate management privilege level. The functions available prior to login – network traffic and warning banner – are configurable, but otherwise the evaluator found no evidence that other function, particularly the management functions, would be available without first logging in.

Guidance Assurance Activities: The evaluator shall review the operational guidance to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of this PP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.

The ST identifies the following as restricted: audit configuration data, information flow policy ACLs, user and administrator security attributes (including passwords and privilege levels), authentication method lists, the logon failure threshold, the remote access user list; and cryptographic support settings.

The following functions are identified in FMT_SMF.1 in the ST: remote and local administration, update the TOE, Configure TOE-provided services available before authentication (routing and warning banner), configure cryptographic functionality.

As such, instructions have been identified by the evaluators for the following list of functions suggested by the ST:

- Audit configuration data
  - The FIPS Configuration Guide includes instructions for "Configure an encrypted syslog server".
  - The Security Configuration Guide includes instructions for "ACL logging".
  - The Administration Guide includes instructions for "Syslog service configuration".
- Information flow policy ACLs
  - The Security Configuration Guide includes instructions for "Rule-Based IP ACLs", "IPv6 ACLs", "IPv6 RA Guard", "802.1X Port Security", "MAC Port Security", "MAC-based VLANs", "Defining MAC Address Filters", and "Multi-Device Port Authentication" that collectively provide instructions for configuring information flow rules.
- User and administrator security attributes (including passwords and privilege levels)
  - The Security Configuration Guide includes instructions for "Local user accounts" that allows user accounts to be defined and assigned password and management privilege levels.
- Authentication method lists
  - Passwords

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

        - The Security Configuration Guide includes instructions for “Local user accounts” that can be used to log into the configured interfaces with an assigned password.
    - SSH public-key based authentication
        - The Security Configuration Guide includes instructions for “Configuring SSH2 client public key authentication”.
- Logon failure threshold
    - The Security Configuration Guide includes instructions for “Setting the number of SSH authentication retries” and “Limiting the number of web authentication attempts”.
- Remote access user list/Remote and local administration
    - The Security Configuration Guide, section 1, addresses local (CLI) and remote access restrictions. Section 2 provides instructions for configuring SSHv2 and SCP.
- Cryptographic support settings/Configure cryptographic functionality
    - The FIPS Configuration Guide provides instructions to enable FIPS and Common Criteria modes.
- Update the TOE
    - The FIPS Configuration Guide includes instructions for “Software Upgrade for FIPS devices”.
    - The Administration Guide includes instructions for “Software versions installed and running on a device”.
    - The Software Upgrade Guide provides comprehensive instructions for upgrading and downgrading the TOE software.
- Configure TOE-provided services available before authentication
    - Network routing
        - The Security Configuration Guide includes instructions for “Rule-Based IP ACLs”, “IPv6 ACLs”, “IPv6 RA Guard”, “802.1X Port Security”, “MAC Port Security”, “MAC-based VLANs”, “Defining MAC Address Filters”, and “Multi-Device Port Authentication” that collectively provide instructions for configuring information flow rules.
    - Warning banner
        - The Security Configuration Guide includes instructions for “Requirement to accept the message of the day”

Testing Assurance Activities: None Defined

2.5.2 Specification of Management Functions (FMT_SMF.1)

2.5.2.1 FMT_SMF.1.1

TSS Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The security management functions for FMT_SMF.1 are distributed throughout the PP and are included as part of the requirements in FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1.

The evaluator was able to use the guidance documentation to configure the TOE to perform the other tests required by the NDPP. All administrator commands are recorded in the audit trail.

2.5.3 Restrictions on Security Roles (FMT_SMR.2)

2.5.3.1 FMT_SMR.2.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.5.3.2 FMT_SMR.2.2

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Testing Assurance Activities: None Defined

2.5.3.3 FMT_SMR.2.3

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.

The **FIPS Configuration Guide** refers to instructions to configure SSHv2 It suggests that in FIPS mode telnet and HTTP are disallowed. In CC mode, HTTPS is also disallowed. The CLI is the default initial interface and no configuration is needed.

The **Security Configuration Guide**, section 1 **Securing Access Methods**, indicates that Serial CLI, telnet, SSH, SNMP, and TFTP. Of these telnet and TFTP are disabled in FIPS mode and SNMP access to critical security parameters is also disabled. Instructions are provided specifically to manage access to the available management interfaces including CLI using a local connection and SSHv2.

Note that the local CI and remote SSH interfaces are identical in that the same commands can be issued in each case.

In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this PP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.

The evaluator performed administration using the console as well as the SSH connection. Both resulted in a command line interface so both were addressed thoroughly.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.6 Protection of the TSF (FPT)

2.6.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1)

2.6.1.1 FPT_APW_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.6.1.2 FPT_APW_EXT.1.2

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note **in the NDPP**.

Section 6.6 states that the TOE does not offer any interfaces that will disclose to any user a plain text password. Additionally, locally defined passwords are not stored in plaintext form.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.6.2 Extended: Protection of TSF Data (for reading of all symmetric keys) (FPT_SKP_EXT.1)

2.6.2.1 FPT_SKP_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note **in the NDPP**. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Section 6.6 states that the TOE does not offer any interfaces that will disclose to any user cryptographic key.

2.6.3 Reliable Time Stamps (FPT_STM.1)

2.6.3.1 FPT_STM.1.1

TSS Assurance Activities: The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time. The TSS provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.

Section 6.6 states the TOE provides a hardware clock for reliable time stamps. The description explains the clock is mainly used for timestamps in audit records but also supports the timing elements of cryptographic functions. By virtue of being a real-time clock, the evaluator assumes it is reliable.

Guidance Assurance Activities: The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the operational guidance instructs

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.

The **Administration Guide** in the **Configuring NTP** section discusses using the set clock command to set the local clock. In the same section, there is an extensive discusses about how to establish communication with an NTP server and how to configure the client. Commands are provided for each topic and examples are given.

Testing Assurance Activities: Test 1: The evaluator uses the operational guide to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.

Test2: [conditional] If the TOE supports the use of an NTP server; the evaluator shall use the operational guidance to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the operational guidance.

The evaluator set the local clock from the console and observed the time change. The evaluator then configured a NTP server and had the appliance connect to the NTP server and update the time. The evaluator observed the time update from the NTP server.

2.6.4 TSF Testing (FPT_TST_EXT.1)

2.6.4.1 FPT_TST_EXT.1.1

TSS Assurance Activities: The evaluator shall examine the TSS to ensure that it details the self tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying 'memory is tested', a description similar to 'memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written' shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

Section 6.6 provides a discussion of the self-tests. When operating in FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing. The module performs Cryptographic algorithm known answer tests, firmware integrity tests using DSA signature verification and conditional self-tests for DRBG, Hardware RNG, Pair-wise consistency tests on generation of RSA keys, and a Firmware load test (DSA signature verification). Upon failing any of its FIPS mode power-on self-tests, the TOE will refuse to boot.

Guidance Assurance Activities: The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

In the **Reloading the device** section of the **FIPS Configuration Guide**, there is a discussion of the FIPS self-tests. This discussion also the possible errors that may arise such as:

- `Crypto module initialization and Known Answer Test (KAT) failed with reason:(Error Code 0x80000000)'CKR_VENDOR_DEFINED'`
- `FIPS: Primary image verification failed`
- `FIPS: Secondary image verification failed`

The TSS description about the self-tests focuses on the FIPS self-tests. As such, the discussion in the **FIPS Configuration Guide** correctly discusses the possible errors that may arise and how to possibly address some of the errors.

Testing Assurance Activities: None Defined

2.6.5 Extended: Trusted Update (FPT_TUD_EXT.1)

2.6.5.1 FPT_TUD_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.6.5.2 FPT_TUD_EXT.1.2

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.6.5.3 FPT_TUD_EXT.1.3

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: Updates to the TOE either have a hash associated with them, or are signed by an authorized source. If digital signatures are used, the definition of an authorized source is contained in the TSS, along with a description of how the certificates used by the update verification mechanism are contained on the device. The evaluator ensures this information is contained in the TSS. The evaluator also ensures that the TSS (or the operational guidance) describes how the candidate updates are obtained; the processing associated with verifying the digital signature or calculating the hash of the updates; and the actions that take place for successful (hash or signature was verified) and unsuccessful (hash or signature could not be verified) cases.

Section 6.6 of the ST discusses TOE software updates. Updates can either be obtained automatically (when so configured) or manually by the administrator using CLI commands. If automatic, the TOE checks for updates when it boots. If manual, the administrator can check for updates using SCP or TFTP. In either case, prior to actually installing and using the new software image, its digital certificate is verified by the TOE using the public key in the certificate configured in the TOE. An unverified image cannot be installed. Note that the TOE comes preinstalled with an applicable Brocade public certificate.

The FIPS Configuration Guide states in Table 2 that TFTP is disabled in FIPS mode. It provides commands for using SCP in Table 3.

The evaluator shall perform the following tests:

Test 1: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that it is successfully installed on the TOE. Then, the evaluator performs a subset of other assurance activity tests to demonstrate that the update functions as expected. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update.

Test 2: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains or produces an illegitimate update, and attempts to install it on the TOE. The evaluator verifies that the TOE rejects the update.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

The Brocade products do not have an update available for testing. Brocade typically does not release small updates or patches. Instead, new firmware versions are released. In order to perform this test, evaluator had to roll back to an engineering version and then roll forward to the released product. The version did update properly. For the improper update, the evaluator attempted to load an image that did not match the signature. The signature verification failed.

2.7 TOE ACCESS (FTA)

2.7.1 TSF-INITIATED TERMINATION (FTA_SSL.3)

2.7.1.1 FTA_SSL.3.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall perform the following test:

Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.

The evaluator set the SSH time period to 2 minutes and observed a SSH timeout. The evaluator then set the SSH timeout to 3 minutes and observed a SSH timeout. Note that when the session terminated, the screen was left as-is and a new login prompt was presented.

2.7.2 USER-INITIATED TERMINATION (FTA_SSL.4)

2.7.2.1 FTA_SSL.4.1

TSS Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall perform the following test:

Test 1: The evaluator initiates an interactive local session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.

The evaluator established both local and remote (SSH) sessions and manually 'exit'ed per the command identified in the guidance. In each case the session was terminated and a logout audit record was logged.

2.7.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

2.7.3.1 FTA_SSL_EXT.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall perform the following test:

Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that re-authentication is needed when trying to unlock the session.

The evaluator set the console time period to 2 minutes and observed a console timeout. The evaluator then set the console timeout to 3 minutes and observed a console timeout. Note that when the session terminated, the screen was left as-is and a new login prompt was presented.

2.7.4 Default TOE Access Banners (FTA_TAB.1)

2.7.4.1 FTA_TAB.1.1

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

TSS Assurance Activities: The evaluator shall check the TSS to ensure that it details each method of access (local and remote) available to the administrator (e.g., serial port, SSH, HTTPS).

Section 6.7 identifies that the administrator can access the TOE using any of the following methods: console or SSH.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: The evaluator shall also perform the following test:

Test 1: The evaluator follows the operational guidance to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.

The evaluator set a login banner and then tested the banner is displayed from the console login as well as an SSH login.

2.8 Trusted path/channels (FTP)

2.8.1 Inter-TSF trusted channel (FTP_ITC.1)

2.8.1.1 FTP_ITC.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.8.1.2 FTP_ITC.1.2

TSS Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.8.1.3 FTP_ITC.1.3

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Section 6.8 indicates that TLS is required to communicate with a SYSLOG server and SCP (based on SSH) is used to communicate with an update server. This is consistent with the choices made in FPT_ITC.1.

The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

The **FIPS Configuration Guide** – Configuring an encrypted syslog server and Appendix A with the same name offer instructions and examples to set up a secure channel to a SYSLOG server.

The **FIPS Configuration Guide** states in Table 2 that TFTP is disabled in FIPS mode. It provides commands for using SCP in Table 3.

The evaluator shall also perform the following tests:

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

a. Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

b. Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.

c. Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.

e. Test 4: The evaluators shall, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Further assurance activities are associated with the specific protocols.

Test 1 – The syslog server communication path was tested as part of setting up the syslog server connection. The update server connection was tested as part of testing an update.

Test 2 - The syslog server communication path (TLS) was tested as part of setting up the syslog server connection. The update server connection (SSH) was tested as part of testing an update.

Test 3 – The establishment of the syslog sever connection ensured the syslog path is encrypted. The evaluators also captured a transfer of an image using scp to ensure the communication path is encrypted.

Test 4 – For both the syslog and update server connections, the evaluator interrupted the communications path. In both case, the connection resumed in an encrypted form. This was verified using Wireshark.

2.8.2 Trusted Path (FTP_TRP.1)

2.8.2.1 FTP_TRP.1.1

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

2.8.2.2 FTP_TRP.1.2

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

2.8.2.3 FTP_TRP.1.3

TSS Assurance Activities: None Defined

Guidance Assurance Activities: None Defined

Testing Assurance Activities: None Defined

Component Assurance Activities: The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

Section 6.8 indicates that SSH is required for remote administration.

The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

The **FIPS Configuration Guide** refers to instructions to configure SSHv2. It states that in FIPS mode telnet and HTTP are disallowed. In CC mode, HTTPS is also disallowed. The CLI is the default initial interface and no configuration is needed.

The evaluator shall also perform the following tests:

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

Test 1: The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. Test 2: For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path. Test 3: The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext. Further assurance activities are associated with the specific protocols.

Test 1 – The evaluator tested SSH when testing the FCS_SSH_EXT.1 requirement.

Test 2 – The evaluator was unable to find a method of using SSH without invoking the trusted path. The communications path was always encrypted and used the servers key.

Test 3 – The evaluator tested the correctness of the SSH encryption when testing the FCS_SSH_EXT.1 requirement.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

3. Protection Profile SAR Assurance Activities

The following sections address assurance activities specifically defined in the claimed Protection Profile that correspond with Security Assurance Requirements.

3.1 Development (ADV)

3.1.1 Basic functional specification (ADV_FSP.1)

Assurance Activities: There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 4.2, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided.

3.2 Guidance documents (AGD)

3.2.1 Operational user guidance (AGD_OPE.1)

Assurance Activities: Some of the contents of the operational guidance will be verified by the assurance activities in Section 4.2 **of the NDPP** and evaluation of the TOE according to the CEM. The following additional information is also required.

The operational guidance shall at a minimum list the processes running (or that could run) on the TOE in its evaluated configuration during its operation that are capable of processing data received on the network interfaces (there are likely more than one of these, and this is not limited to the process that 'listens' on the network interface). It is acceptable to list all processes running (or that could run) on the TOE in its evaluated configuration instead of attempting to determine just those that process the network data. For each process listed, the administrative guidance will contain a short (e.g., one- or two-line) description of the process' function, and the privilege with which the service runs. 'Privilege' includes the hardware privilege level (e.g., ring 0, ring 1), any software privileges specifically associated with the process, and the privileges associated with the user role the process runs as or under.

The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

The documentation must describe the process for verifying updates to the TOE, either by checking the hash or by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

1. For hashes, a description of where the hash for a given update can be obtained. For digital signatures, instructions for obtaining the certificate that will be used by the FCS_COP.1(2) mechanism to ensure that a signed update has been received from the certificate owner. This may be supplied with the product initially, or may be obtained by some other means.

2. Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).

3. Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature..

The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.

The **FIPS Configuration Guide** has been updated in the Overview section to state that in FIPS mode, the network processing occurs in the kernel and in privileged daemons. Note that the product goes into FIPS mode prior to going into CC mode.

The **FIPS Configuration Guide** includes an Appendix C that provides tables that list the running tasks for the different FastIron devices in FIPS mode. These tables list the task name, priority, and provide a brief description.

The product updates are digitally signed by Brocade. The appliance verifies each imagine when loaded. To obtain an update, the user is instructed to download the required software images from the Downloads page in MyBrocade web site. The **FIPS Configuration Guide** provides detailed instructions for copying the new signature and new imagine onto the device and loading the new signature image. The steps discuss where to put the image and the commands to install it. The steps also verify the signature. A list of potential error message is described and some troubleshooting tips are included in case the upgrade fails.

3.2.2 Preparative procedures (AGD_PRE.1)

Assurance Activities: As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

The evaluator can access Hardware Installation Manuals for all product families - SX, ICX, and FCX online at www.brocade.com. The more general manuals like **FIPS Configuration Guide** and the **Security Configuration Guide** apply to all models. The completeness of the manuals is addressed by their use in the AA's carried out in the evaluation.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

3.3 Life-cycle support (ALC)

3.3.1 Labelling of the TOE (ALC_CMC.1)

Assurance Activities: The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the STFurther, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines in the Brocade Lab used for testing.

3.3.2 TOE CM coverage (ALC_CMS.1)

Assurance Activities: The 'evaluation evidence required by the SARs' in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

See 3.3.1 for an explanation of how all CM items are addressed.

3.4 Tests (ATE)

3.4.1 Independent testing - conformance (ATE_IND.1)

Assurance Activities: The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a 'fail' and 'pass' result (and the supporting details), and not just the 'pass' result.

The evaluator created a Detailed Test Report (DTR) to address all aspects of this requirement. The DTR discusses the test configuration, test cases, expected results, and test results.

3.5 Vulnerability assessment (AVA)

3.5.1 Vulnerability survey (AVA_VAN.1)

Assurance Activities: As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in network infrastructure devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.

boot-up, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and a port scan. Nether the public search for vulnerabilities or the port scan uncovered any residual vulnerability.

© 2014 Gossamer Security Solutions, Inc.
All rights reserved.